CONTENTS

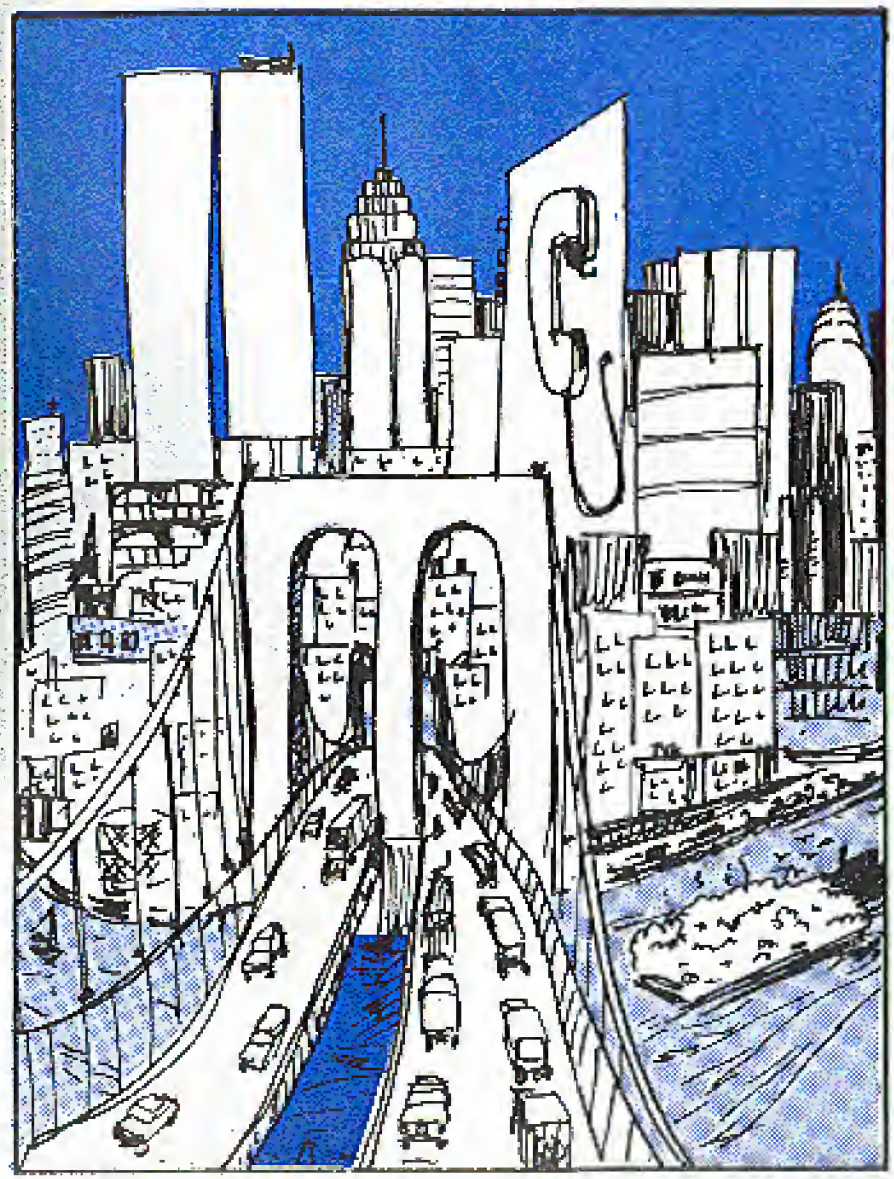
2600 Magazine
PO Box 752
Middle Island, NY 11953 U.S.A.

WARNING:
MISSING LABEL

2600

The Monthly Journal of the American Hacker

Volume 4, Number 7 July, 1987 $2



If you've just opened this magazine, you may want to glance over to your left. That is the beginning of an advertisement for something that many of you have been asking about—2600 back issues. They've always been available in the past, but now we've had our entire collection reprinted to prevent us from running out for a very long time.

Having all of these back issues floating around has been an uplifting experience for us. It's easy to lose track of the many different subjects we've tackled in these pages and it's really amazing to look back on what we've done.

2600 is not like other magazines. Our readers are constantly referring back to previous issues as if they'd just come out, asking questions about certain articles. And in reading over them ourselves, we can understand why. It all seems so fresh and new, even though some of it is three years old and the circumstances have changed.

But one thing that hasn't changed is our feeling towards technological enthusiasts. They understand at least some of what's going on in the world of computers and phones and the average person wants to know what they find out. Most folks would have never heard of TRW Credit Services if it weren't for hackers, let alone know that huge credit files existed in their names. More people wouldn't know what electronic and

(continued on page 2

STAFFBOX

Editor and Publisher
Eric Corley 110

Office Manager
Fran Westbrook

Cover Art
Tish Valter Koch

Writers: John Drake, Paul Estev, Dan Foley, Mr. French, Emmanuel Goldstein, Chester Holmes, The Kid & Company, Lex Luthor, Bill from RNOC, David Ruderman, Bernie S., Mike Salerno, Silent Switchman, Mike Yuhas, and the usual anonymous bunch.

Production: Mike DeVoursney.
Cartoonists: Dan Holder, Mike Marshall.
Editor Emeritus: TSH.

2600 (ISSN 0749-3851) is published monthly by 2600 Enterprises, Inc. 7 Strong's Lane, Setauket, NY 11733. Second class postage permit pending at Setauket, New York.

POSTMASTER: Send address changes to 2600, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada—$15 individual, $40 corporate.
Overseas—$25 individual, $55 corporate.
Back issues available at $25 per year, $30 per year overseas.
ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO: 2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752.
For letters and article submissions, write to: 2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0752.

Cellular Phone Fraud and Where It's Headed

by Bernie S.

The recent FBI/Secret Service cellular sting operation that culminated in the arrests of over 25 people in New York City confirms what many of us have suspected for quite some time: that cellular telephone fraud is widespread. The FBI estimates that cellular phone fraud costs system operators $3 million anually; with the average subscriber's airtime bill about $50 per month for 100 minutes of usage, there could be over 2500 cellular pirates on the air if a pirate uses twice the normal amount of airtime. The term "pirate" rather than "phreak" is used here because the vast majority of illegitimate CMT users (Cellular Mobile Telephone) are only interested in stealing airtime, while phone phreaks are mainly interested in learning more about the telephone network through its manipulation.

The six-month FBI investigation used "cooperative sources" who named fraudulent installers; then FBI agents posing as customers and installers used standard entrapment techniques to gather evidence against those allegedly involved. The FBI's press release statement that "recent technological advances in computerized telephone switching equipment and billing systems were instrumental in...(their investigation)" is deliberately misleading. New York cellular carrier NYNEX merely supplied the FBI with its billing data to document the use of bogus and stolen ESN's & MIN's (Electronic Serial Numbers and Mobile Identification Numbers) discovered in the investigation. The Secret Service later became involved because the laws relating to the credit fraud being allegated are under their jurisdiction.

Safe Phreaking

In practice, cellular phreaking is very safe if one does their own tranceiver modifications, changes ESN's & MIN's regularly, and uses standard phone phreak precautions. Indeed, FBI agent Greg Meecham has stated that fraudulently programmed CMT's are "unattributable, unbillable, untraceable and untappable." A cellular carrier will become aware of any bogus or stolen ESN's and MIN's used on its system within a month or so after their initial use once the subscriber or carrier who is assigned those codes is billed and notifies them of the error. The home carrier will then change the legitimate subscriber's MIN in the MTSO (Mobile Telephone Switching Office) and arrange for a new NAM (Number Assignment Module, or ROM) to be installed in that subscriber's CMT transceiver. The MTSO maintains a database of all its valid ESN/MIN pairs, as well as a "negative verify" file on all known invalid numbers for the deadbeats and pirates in its area. The carrier may choose to leave certain fraudulent codes active to have any activity monitored, but as long as all parties at the receiving end of any phreaked calls become amnesiac to any inquiries, the phreak's identity will remain secret. If a phreak uses a different ESN & MIN every month, it'll be extremely difficult for the carrier to react in time to gather any information.

As with any landline, inband signalling (i.e. 2600 Hz, MF tones, etc.) will work but can be easily detected by the ESS controlling that line. Since all cellular systems are in metropolitan areas, it's logical to assume that most cellular lines are on ESS. Although telco security may be aware of any blue-boxing, the links in their security chain stop at the MTSO. Moreover, since the MTSO selects outgoing landlines from a trunk group, a pen register at the CO would be useless for establishing any toll fraud patterns.

Because of cellular's inherent frequency-hopping nature, it is very difficult to track down a CMT using conventional radio direction-finding (DF) techniques, even if it's stationary. A small directional antenna aimed randomly at surrounding cell-site repeaters with a TV antenna rotor will thoroughly confuse any DF attempts, although keeping calls as short as possible is always a good precaution. Locating a mobile CMT is virtually impossible. I was recently given a tour of an FCC monitoring van in Washington DC, and was surprised to see how lacking in sophistication their onboard DF gear was. The only equipment available to readily locate a CMT transmitter is primarily used by the military and intelligence agencies, which couldn't care less about CMT fraud unless it involved national security.

Equipment

Most CMT's are actually two main pieces of equipment: the transceiver and control head. The transceiver (transmitter/receiver) is usually a nondescript metal box with three external connectors and contains sophisticated circuitry. There are usually two main circuit boards inside: an RF board with all the radio transmitting/-receiving circuits, and a logic board with a microprocessor, A/D and D/A circuits, and control logic. The control head is a touch-tone telephone handset with an extended keypad, numeric, or alphanumeric display, and volume and mic mute controls. It often has a separate speaker mounted in the cradle for on-hook dialing and call-progress monitoring. Some CMT's have a speakerphone option that allows you to drive with both hands on the wheel by talking into a small microphone mounted near the vehicle's sun visor, and listening to the cradle loudspeaker. This may seem to be the ultimate in laziness, but remember you could be maneuvering your five-speed through heavy traffic on the expressway when the phone rings! The control head/cradle is usually bolted to the transmission hump by the driver's seat, and the transceiver is usually mounted in the trunk with a power cable connecting it to the car battery and ignition switch. A shielded control cable links this equipment together and allows data and audio to pass between them. Most first-generation CMT's used the AMPS bus, developed by AT&T, which specified a system of 36 parallel wires in a bulky control cable. Some manufacturers later developed their own buses—Novatel's serial bus specifies a thin cable of just a few wires which is much easier to install in vehicles. For fixed use, a CMT may be powered by any 12-volt regulated DC power supply that can deliver at least 5 Amperes.

Any would-be cellular phreak must first obtain a CMT. Used bargains abound in some cities, where many subscribers found they couldn't afford to pay their airtime bills after they bought their phone! First-generation E.F. Johnson transceivers are a good choice because they're easy to work on, use a uniquely effective diversity (dual-antenna) receiver, and use the AMPS control bus, which means that several manufacturers' control heads will work with it. Another good choice is Novatel's Aurora/150 model. It uses a proprietary parallel bus and control head, but costs less, is very rugged, and is also easy to work on. In addition, all Novatel CMT's have built-in diagnostics which allow (among other things) manual scanning of all 666 repeater output frequencies—great entertainment when you're bored!

Antennas

A mobile cellular antenna is usually a short (less than a foot long) piece of stiff wire with a half-dozen or so turns in the middle, like a spring. The "spring" acts as a phasing coil in a 5/8-wave configuration. The antenna is mounted vertically either through a hole in the vehicle's roof or at the top of the rear windshield using silicon adhesive with conductive plates on either side to pass RF energy right through the glass. It's not quite as efficient as a roof mount, but most folks prefer not to drill a hole in their Mercedes. A 50-Ohm coaxial cable such as RG-58/U links the antenna to the transceiver with a male TNC-type UHF connector. A ceramic duplexer allows the transmitter and receiver to share the same antenna simultaneously. Mobile roof-mount antennas are designed to work with the ground plane provided by the vehicle's body, but for fixed use an "extended-feed" or voltage-fed coaxial antenna (which requires no ground plane) can be used if there's no tin roof on your house. A capped PVC pipe makes an ideal rooftop housing for this type of antenna, concealing it and making it weatherproof at the same time. As with any kind of antenna, the higher the better—but unless you're surrounded by tall steel buildings any height will probably do (provided you're within range of a cell-site repeater). It should even work indoors if near a window—remember that cellular systems are designed to work primarily with inefficient antennas at ground-level. Yagi and corner-reflector antennas are available for fixed use that provide very high gain and directivity. Antenna specialists Co. (216-791-7878) manufactures a broad line of cellular antennas.

Interfacing

Interfacing audio devices such as MF tone-generators to a CMT can be accomplished by coupling the device's output through an audio coupling transformer and capacitor across the

(continued on page 11)

how phone phreaks are caught

by No Severence

Until about four months ago, I worked in a switchroom for a large long distance company. I was given the pink slip because some guy in my office found out that I did a little hacking and phreaking in my spare time. It seems that most companies just aren't into that anymore. I feel I should do all I can to keep phreaks from getting caught by the IC's (Independent Carriers or Inter-exchange Companies). Remember: a safe phreak is an educated phreak.

When you enter an authorization code to access a long distance company's network there are a few things that happen. The authorization code number you enter is cross referenced in a list of codes. When an unassigned code is received the switch will print a report consisting of the authorization code, the date and time, and the incoming trunk number (if known) along with other miscellaneous information.

When an authorization code is found at the end of a billing cycle to have been abused, one of two things is done. Most of the time the code is removed from the database and a new code is assigned. But there are times when the code is flagged "abused" in the switch. This is very dangerous. Your call still goes through, but there is a bad code report printed. (This is similar to an unassigned code report, but it also prints out the number being called.) You have no way to know that this is happening but the IC has plenty of time to have the call traced. This just goes to show that you should switch codes on a regular basis and not use one until it dies.

Access

There are several ways to access an IC's network. Some are safe and some can be deadly.

Feature Group A (FGA). This is a local dial-up to a switch. It is just a regular old telephone number (for example 871-2600). When you dial the number it will ring (briefly) and give you a dialtone telling you to proceed. There are no identifying digits (i.e. your telephone number) sent to the switch. The switch is signalled to give you a dialtone from the ringing voltage alone. The only way you could be caught hacking codes on an FGA number would be if Telco (your local telephone company) were to put an incoming trap on the FGA number. This causes the trunk number your call came over to be printed out. From the trunk number Telco could tell which central office (CO) your call was coming from. From there Telco could put an outgoing trap in your CO which would print the telephone number of the person placing a call to that number—that is provided that you are in an ESS or other electronic switch. This is how a majority of people are caught hacking codes on an FGA access number.

Next down the line we have **Feature Group B (FGB).** There are two FGB signalling formats called FGB-T and FGB-D. All FGB's are 950-XXXX numbers and I have yet to find one that doesn't use FGB-T format.

When you dial an FGB number your call can take two paths: 1) Large CO's have direct trunks going to the different IC's. This is more common in electronic offices. 2) Your call gets routed through a large switch called a tandem, which in turn has trunks to all the IC's.

When you dial an FGB-T number the IC's switch receives:

KP + ST

This prompts the switch to give you a dialtone. The IC gets no information regarding your telephone number. The only thing that makes it easier to catch you is that with a direct trunk from your central office, when you enter a bad code the IC knows what office you're coming from. Then it's just a matter of seeing who is calling that 950 number.

On the other hand, when you dial an FGB-D number the switch receives:

KP + (950-XXXX) + ST followed by

KP + 0 + NXX-XXXX + ST or **KP + 0 + NPA NXX-XXXX + ST**

The first sequence tells that switch that there is a call coming in, the 950-XXXX (optional) is the same 950 number that you call. The second sequence contains your number (ANI—Automatic Number Identification). If the call comes over a trunk directly from your CO it will not have your NPA (area code). If the call is routed through a tandem it will contain your NPA. FGB-D was originally developed so that when you got the dialtone you could enter just the number you were calling and your call would go through, thus alleviating authorization codes. FGB-D can also be used as FGB-T, where the customer enters a code but the switch knows where the call is coming from. This could be used to detect hackers, but has not been done, at least not in my switch.

FGB-D was the prelude to **Feature Group D (FGD).** FGD is the heart of equal access. Since FGD can only be provided by electronic offices, equal access is only available under ESS (or any other electronic office). FGD is the signalling used for both 1+ dialing (when you choose an IC over AT&T) and 10XXX dialing (see equal access guide, *2600*, March 1987). The signalling format for FGD goes as follows:

KP + II + 10D(10 digits) **+ ST** followed by

KP + 10D + ST

The first sequence is called the identification sequence. This consists of KP, information digits (II), and the calling party's telephone number with NPA (10D ANI) finished up with ST. The second or address sequence has KP, the called number (10D) followed by ST. There is a third FGD sequence not shown here which has to do with international calling—I may deal with this in a future article. When the IC's switch receives an FGD routing it will check the information digits to see if the call is approved and if so put the call through. Obviously, if the information digits indicate the call is coming from a coin phone, the call will not go through.

This is a list of information digits commonly used by Bell Operating Companies.

Code	Sequence	Meaning
00	Identification	Regular line, no special treatment
01	Identification	ONI (Operator Number Identification) multiparty lines
02	Identification	ANI failure
06	Identification	Hotel or Motel
07	Identification	Coinless, hospital, inmate, etc.
08	Identification	InterLATA restricted
10	Address	10X test call
13	International	011-plus: direct distance dialed
15	International	01-plus: operator assisted
27	Identification	Coin
68	Identification	InterLATA-restricted hotel or motel
78	Identification	InterLATA-restricted hospital, coinless, inmate, etc.
95	Address	950-XXXX test call

There is a provision with FGD so when you dial 10XXX# you will get a switch dialtone as if you dial a 950. Unfortunately, this is not the same as dialing a 950. The IC would receive:

KP + II + 10D (ANI) + ST

KP + ST

The KP + ST gives you the dialtone, but the IC has your number by then.

800 Numbers

Now that we have the feature groups down pat we will talk about 800 numbers. Invisible to your eyes, there are two types of 800 numbers. There are those owned by AT&T—which sells WATS service. There are also new 800 exchanges owned by the IC's. So far, I believe only MCI, US Sprint, and Western Union have bought their own 800 exchanges. It is very important not to use codes on 800 numbers in an exchange owned by an IC. But first...

When you dial an AT&T 800 number that goes to an IC's switch the following happens. The AT&T 800 number is translated at the AT&T switch to an equivalent POTS (Plain Old Telephone Service). This number is an FGA number and as stated before does not know where you're calling from. They might know what your general region is since the AT&T 800 numbers can translate to different POTS numbers depending on where you're calling from. This is the beauty of FGA and AT&T WATS but this is also why it's being phased out.

On the other hand, IC-owned 800 numbers are routed as FGD calls—very deadly. The IC receives:

KP + II + 10D + ST

KP + 800 NXX XXXX + ST

When you call an IC 800 number which goes to an authorization code-based service, you're taking a great risk. The IC's can find out very easily where you're calling from. If you're in an electronic central office your call can go directly over an FGD trunk. When you dial an IC 800 number from a non-electronic CO your call gets routed through another switch, thus ending up with the same undesirable effect.

MCI is looking into getting an 800 billing service tariffed where a customer's 800 WATS bill shows the number of everyone who has called it. The way the IC's handle their billing, if they wanted to find out who made a call to their 800 number, that information would be available on billing tapes. The trick is not to use codes on an

(continued on page 10)

the telecom informer

BY GOLDSTEIN

If you're in New Orleans, a simple seven-digit number can wind up costing you $25. That's right, if you call 976-2767, a $25 charge is added to your bill. The money is then donated to the New Orleans Symphony to help them pay off a $3.8 million debt. Seems like it won't be too hard to *run up* a $3.8 million debt of your own with this trick. By the way, if you call it from out of the area (area code 504), you'll hear the same thank-you message, but you won't get charged anything more than a long-distance call. Classical music lovers: if you have some extenders in New Orleans, you could quickly put these guys back in the black! Only kidding....Bell of Pennsylvania is going to initiate a service that would allow customers to hang up during the first 10 seconds of a dial-it service message and not get charged. The first 10 seconds will be a warning, both of the price of the service and of the possibly offending content....Have you signed up recently for long distance service from California Discall or Hello America? If so, then you were involved in telephone fraud! California Discall, also known as Lindahl Enterprises, allegedly sold flat-rate long distance service to hundreds of businesses nationwide, then distributed stolen US Sprint access codes to its customers. Sprint was also used by Hello America, which reportedly billed them for $3,018,818 as of January. You have to wonder why Sprint always seems to be the victim of these schemes. Perhaps they could work it into their ads—"Sprint: the choice of thieves." Speaking of which, common criminals are getting into the act with a vengeance. You can buy stolen Sprint and MCI codes on the street, for up to $400. (This, incidentally, is a rotten deal—they usually go bad within a day.) You might also run across a clandestine "operator" who will place your call for you and charge you several dollars on the spot....Robert Post of Poland allegedly robbed $86,000 from New York ATM machines and he did it without stealing cards. He'd simply look over customers' shoulders as they were conducting transactions and memorize their PIN code. Then, if the customers didn't take their receipt (mirrors), Post would snatch it up and get the card number. Then, using a special machine, Post would create his own version of their cards, complete with a magnetic strip with pertinent information. He also needed the Manufacturers Hanover "signature" that is imbedded on the strip, which apparently has leaked out. His method worked, but it consistently set off alarms and that is how he was caught....A new computer system is working hard in New York State to find fathers who are delinquent in child-support payments. Computers at two state agencies are now talking to each other, allowing a match to be made between the offender and his employer. The employer is ordered to withhold whatever is overdue from the person's paycheck....Nobody understands why New York Telephone embarked on a hopeless campaign of plastering pay phones with little blue stickers that said "New York Telephone, A Nynex Company" on them. Perhaps they're suffering from an identity crisis and want Nynex phones to stand out from all the others, some of which look remarkably similar. But these stickers were so easy to peel off that they had been appearing everywhere except on Nynex phones—cars, bicycles, refrigerators, even other pay phones that obviously *aren't* Nynex phones. Almost as quickly as they appeared, all of the remaining stickers vanished. Now there are huge signs on top of all the phones that identify them as the precious Nynex models. They've also replaced all of the faceplates on the front of the phones. They sure do keep busy at Nynex, don't they?

(continued on page 16)

An Exciting 2600 Contest

DIFFERENT WAYS TO ANSWER THE PHONE

Tired of just plain "Hello"? So are we. Send us your ideas on what to holler when the ringer jingles. We'll give the best entry a TWO-YEAR subscription to *2600*!

NOT EVERYONE HAS TO USE "HELLO". HERE ARE SOME ALTERNATIVES....

"Suicide Hotline, please hold...."
"Yes, Commissioner."
"Operator, may I help you?"
"Wrong number."
"Authorization code, please?"
"Bueno!"

CONTEST RULES: No more than 3 entries per contestant, please. Entries must be received by September 1, 1987. Entries will be judged primarily on brevity and levity, but other outstanding merits including assonance, dissonance, alliteration, allusion, or shock value will be considered. Deserving entries will be printed in an upcoming issue of 2600 WITHOUT contestants' names, unless entry includes the request "Please attribute to (name or handle)". All judgements are final. Winner will receive a 2-year subscription or extension to their existing subscription. Runner(s)-up will receive a 1-year subscription or extension.

SEND ENTRIES TO:
2600 CONTEST
PO BOX 99
MIDDLE ISLAND, NY 11953-0099

how phone phreaks get caught

(continued from page 7)

IC-owned 800.

The way to find out who owns an 800 exchange is to call 800-NXX-0050 (NXX being the 800 exchange). If this is owned by AT&T you will get a message saying, "You have reached the AT&T Long Distance network. Thank you for choosing AT&T. This message will not be repeated." When you call an exchange owned by an IC you will usually get a recording telling you that your call cannot be completed as dialed, or else you will get a recording with the name of the IC. If you call another number in an AT&T 800 exchange (i.e. 800-NXX-0172) the recording you get should always have an area code followed by a number and a letter, for example, "Your call cannot be completed as dialed. Please check the number and dial again. 312 47." As of last month, most AT&T recordings are done in the same female voice. An MCI recording will tell you to "Call customer service at 800-444-4444" followed by a switch number ("MCI 205").

Some companies, such as US Sprint, are redesigning their networks. Since the merger of US Telecom and GTE Sprint, US Sprint has had 2 separate networks. The US Telecom side was Network 1 and the GTE side was Network 2. US Sprint will be joining the two, thus forming Network 3. When Network 3 takes effect there will be no more 950-0777 or 10777. All customers will have 14 digit travel cards (referred to as FON cards, or Fiber Optic Network cards) based on their telephone numbers. Customers who don't have equal access will be given seven digit "home codes". These authorization codes may only be used from your home town or city. The access number they will be pushing for travel code service will be 800-877-8000. This cutover was supposed to have been completed by June 27 but the operation has been pushed back.

One last way to tell if the port you dialed is in an IC's 800 exchange is if it doesn't ring before you get the tone. When you dial an FGA number it will ring shortly but when you dial 10XXX# you get the tone right away. Last but not least, I will provide you with a list of 800 exchanges that are owned by IC's. A majority of them are owned by MCI.

MCI

800-234 800-274 800-283 800-284 800-285
800-293 800-333 800-365 800-444 800-456
800-627 800-666 800-678 800-727 800-759
800-777 800-825 800-876 800-888 800-937
800-950 800-955 800-999

US Sprint

800-347 800-366 800-699 800-877

Western Union

800-368

And to avoid confusion, these are the AT&T 800 exchanges:

800-202 800-212 800-221 800-222 800-223
800-225 800-227 800-228 800-231 800-232
800-233 800-235 800-237 800-238 800-241
800-242 800-243 800-245 800-247 800-248
800-251 800-252 800-253 800-255 800-257
800-258 800-262 800-263 800-265 800-267
800-268 800-272 800-282 800-292 800-302
800-312 800-321 800-322 800-323 800-325
800-327 800-328 800-331 800-332 800-334
800-336 800-338 800-341 800-342 800-343
800-344 800-345 800-346 800-348 800-351
800-352 800-354 800-356 800-358 800-361
800-362 800-363 800-367 800-368 800-372
800-382 800-387 800-392 800-402 800-412
800-421 800-422 800-423 800-424 800-426
800-428 800-431 800-432 800-433 800-435
800-437 800-438 800-441 800-442 800-443
800-445 800-446 800-447 800-448 800-451
800-452 800-453 800-457 800-458 800-461
800-462 800-463 800-465 800-466 800-471
800-482 800-492 800-502 800-512 800-521
800-522 800-523 800-524 800-525 800-526
800-527 800-528 800-531 800-532 800-533
800-535 800-537 800-538 800-541 800-542
800-543 800-544 800-545 800-547 800-548
800-551 800-552 800-553 800-554 800-555
800-556 800-558 800-561 800-562 800-563
800-565 800-567 800-572 800-582 800-592
800-602 800-612 800-621 800-622 800-624
800-626 800-628 800-631 800-632 800-633
800-634 800-635 800-637 800-638 800-641
800-642 800-643 800-645 800-647 800-648
800-652 800-661 800-661 800-662 800-663
800-665 800-667 800-672 800-682 800-692
800-702 800-712 800-722 800-732 800-742
800-752 800-752 800-772 800-782 800-792
800-802 800-812 800-821 800-822 800-824
800-826 800-828 800-831 800-832 800-833
800-835 800-841 800-842 800-843 800-845
800-847 800-848 800-851 800-852 800-854
800-855 800-858 800-862 800-872 800-874
800-882 800-892 800-902 800-912 800-922

(continued on page 20)

CELLULAR FRAUD

(continued from page 5)

control head's microphone wires. If it's available, a schematic diagram will show which CMT bus lines carry the transmit audio; coupling the signal there would be preferable. Acoustic modems can be interfaced acoustically, or by coupling the mic and speaker wires to those on the control head or to the appropriate bus lines. Direct-connect modems, answering machines, regular and cordless telephones, and other devices can be interfaced to a CMT through the ABTX cellular interface manufactured by Morrison & Dempsey Communications (818-993-0195). This $300 device is a one-line PBX that connects between the transceiver and control head and provides an RJ-11C jack that accepts any direct-connect telephone accessory. It recognizes touch-tone and pulse dialing, provides 1.0B equivalent ringing voltage, and generates dial and busy tones when appropriate.

Access Codes

Every CMT manufactured has a unique ESN, which is a four-byte hexadecimal or 11-digit octal number in a ROM soldered directly to the logic board. It's supposed to be there for life and never removed. Some newer CMTs imbed the ESN in a VLSI chip along with the unit's program code, which makes ESN modifications virtually impossible. The ESN is also imprinted on the receiver ID plate mounted on the outside housing. When converted to octal (11 digits), the first three digits specify the CMT manufacturer, and the other 8 identify the unit. Typical ESN's might be 13500014732 (octal) for a NEC brand CMT, and 8E01A7F6 (hexadecimal) for a Novatel. The other important chip is the NAM, which contains the MIN (NPA-XXX-XXXX), lock code (keeps the kids from using it), and various model-specific and carrier-specific codes. Some newer CMTs have no NAM at all and use an EEPROM which allows a technician who knows the maintenance code to change NAM data through the control head keypad.

Basically, when one attempts to make a CMT call the transceiver first automatically transmits its ESN and NAM data to the nearest cell-site repeater by means of the overhead data stream, or ODS. The ODS is a 10 kilobaud data channel that links the CMT's computer to the MTSO computer, which controls the phone's entire operation right down to its channel and RF output power. If the MTSO doesn't recognize the received ESN/MIN pair as valid, it returns a reorder signal and will not process the call. In most cities with cellular systems there are two carriers: the wireline operator (usually Bell or the local telco) and the non-wireline operator, an independant company. Both maintain their own MTSO and network of cell-site repeaters, and occupy separate halves of the cellular radio band. Non-wirelines operate on system A (channels 001 to 333), and wirelines on system B (channels 334 to 666).

Custom-Calling features such as call-forwarding, call-waiting, and three-way calling are all standard with most cellular carriers, but the procedures for using them differ so it's best to call the carrier for more information.

Obtaining Codes

The most difficult task for cellular phreaks and pirates is obtaining usable ESN's and MIN's. One method involves having an accomplice who is employed at a CMT installation center. They will have a file on every CMT installed at that location, including the ESN's and MIN's assigned to those subscribers. Using several codes from one source could focus attention there, however. Another method involves the help of an inside person at the cellular carrier's customer service or billing department, where many low-paid employees have access to thousands of valid ESN's and MIN's. The most sophisticated method requires interfacing a CMT's A/D circuitry to a personal computer, enabling one to literally pick valid codes out of thin air.

Programming the CMT

Once a valid ESN/MIN pair is obtained, it must be programmed into the CMT's ROM's. Some CMT manufacturers use different devices and memory maps, but most adhere to the AMPS 16-pin, 32x8 bit format. The most common ROM's are Signetics 82S23 (open collector) and 82S123 (tri-state) or equivalents, but it's best to check the part number's used in your unit. The existing ESN ROM should be carefully removed from the logic board using grounded desoldering tools and read using a NAM programmer's bit-editor mode. Any PROM programmer that is device-compatible can be used, but dedicated

(continued on page 14)

The Letters

On Disclaimers

Dear *2600*:

In the July 1984 issue of *2600*, Quasi Moto, sysop of the late Plover-Net BBS said he had the "perfect" disclaimer for a BBS. I have some friends who are starting a BBS, and they could *really* use his "perfect" disclaimer.

MAC???

There is no such thing. Many computer bulletin boards ask the question, "Are you a member of the law enforcement community?" And members of the law enforcement community simply answer in the negative. You won't find many judges who will sympathize with a defendant that was "lied to" by a cop. Other boards claim they're not responsible for anything that's posted by others. Well, that may be so, but if the law this month says sysops are responsible, they will feel the heat, disclaimer or no disclaimer. So what are we saying? Disclaimers are useless and offer a false sense of security. In many cases they do more harm than good because the very presence of a disclaimer leads some to believe that something illegal is going on. You're better off running a board you can be proud of and whose contents you're prepared to defend. It being the 80's, you may very well have to justify your existence.

Texas Toll Fraud

Dear *2600*:

Enclosed is a tabloid article about access code toll fraud on Texas college campuses. Hope you guys get some use or laughs from it.

It mentions a number set up by Texas Tech for students to turn themselves in for toll fraud. Has anyone ever considered doing the following?

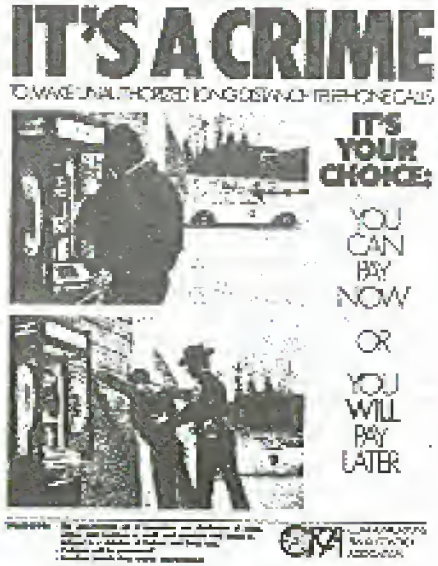
"Hello, (insert name of long distance company)? I would like to turn myself in for toll fraud. My name is (insert name of some person you wish revenge on)."

You can guess what happens from there....

Technocracy now!

The Hooded Claw

What you suggest is immoral, unjust, sneaky, disgusting, and horrible. It's also incomplete. The number to call is 703-641-9292. It belongs to the Communications Fraud Control Association, that scary organization that gathers information from all of the long distance companies. They recently plastered Texas Tech with posters, a likeness of which appears on this page.



Suggestions, Comments

Dear *2600*:

Can you tolerate another comment on the new format vs. 3-ring binder compatibility? Add an enticing centerfold picture. Maybe then your readers would realize that *opened*, the new format is really the 3-ring binder format "sort of on its side". Some creative hole punching, and, by golly, the new format fits in a 3-ring binder! (You can help, of course, by leaving a bit more margin at the top of the new page format.)

Now what do I do with my address labels? I just recently tried the "new Private Sector bulletin board" advertised on the January and February back covers. Why no answer at 201-366-4431?

How about an updated list of private BBS numbers? Especially in the Western part of the country. Anyone in the Los Angeles area have any good ones to share?

The RAM

Not a bad idea for hole placement. At the moment, though, it's not a viable option for us.

The entire hole controversy has really gotten out of hand. Is it so hard to file something away that doesn't have holes in it? Let's see if we can come up with creative ideas for doing just that.

Private Sector will not be coming back up, unfortunately. But we are planning an active BBS future for our readers. Response to last month's appeal for BBS's nationwide has been encouraging. What you will soon see is a list of bulletin boards that have agreed to be "2600 bulletin boards". Each will have its own unique traits, but will also possess certain key similarities and functions. We are in the process of determining what the common denominators should be. Please send us your input on this.

A Horrible Problem

Dear *2600*:

I have a rather specific communications problem. Let me hasten to add that I am seeking a completely legal solution, as I do not wish to become involved in an international incident!

The problem is that I want to transmit computer data from one location to another—specifically, I want to be able to access a computer BBS from my home location, about five miles away. But, I want to be able to do this without incurring per-minute toll charges. The sysop is a friend of mine and would probably be able to connect the computer to a radio link during the time I wish to use it, but there is one further problem—not only is the BBS a long distance call from my location; it also happens to be on the other side of an international border, in Sault Ste. Marie, Ontario, Canada.

I realize that one possible solution would be to use amateur packet radio, but neither my friend nor I are amateurs, nor, quite frankly, do we have any desire to become ham radio operators. We have three big objections to amateur radio—first, we don't want to waste time trying to learn the antiquated morse code; second, we have met far too many amateurs who seem to think of amateur radio as their personal fraternity, and who are far too willing to make trouble for those who don't share their views on how things should be done; and third, the BBS often contains messages of computer equipment wanted or for sale, and I suspect that these would be considered business-related transmissions by the FCC and thus could not be legally transmitted over amateur radio (and it would be impractical to try and segregate those types of messages from the rest of the message base).

If the distance involved were longer, I would suppose that we are probably stuck with Ma Bell, but due to the short distance I can't help but think there must be some way to avoid the toll. My friend and I can easily talk for hours via CB radio (although it would be nice to have a somewhat more private link and no "skip" interference), but it is my

(continued on page 18)

Never Stop

CELLULAR FRAUD

(continued from page 11)

NAM programmers have built-in software which greatly simplifies the process. The ESN printed on the ID plate (if in decimal, convert to hex) should be found in memory and will be immediately followed by an 8-bit checksum determined by the 8 least significant bits of the hex sum of the ESN's four bytes. The old ESN data (now copied into the NAM programmer's RAM) should be replaced with the new ESN and checksum. A new blank ROM of the same type should be inserted into the programmer and "burned." It would be advisable to solder a ZIF (Zero Insertion Force) DIP socket onto the logic board to accomodate the new ESN chip and any future versions.

The NAM chip is usually already ZIF socketed on the logic board for easy replacement. It, too, should be copied into the NAM burner's RAM and the old MIN replaced with the new one. The NAM checksum should also be updated to reflect the new data. Although the carrier's system parameters must also be programmed into the NAM, they can be left the same if the NAM being changed had previously been on the carrier now to be used. All that needs to be changed in this case is the last four MIN digits and checksum (and maybe the exchange if they're using more than one). An excellent write-up on NAM programming is available free of charge from Curtis Electro Devices (415-964-3346). Ask for the May '87 reprint from Cellular Business magazine. Bytek Corporation (305-994-3520) sells a good budget NAM programmer for about $500, and the operations manual (available separately) explains in detail the memory maps, part numbers, and programming techniques for most CMT's on the market. This same unit is also capable of programming many ESN chips using the bit-editor mode. Some carriers and their installation agents will provide NAM system parameters on request, and some CMT service facilities will provide NAM and ESN memory maps and schematics of specific CMT's for a price.

One could eliminate the need for a NAM programmer altogether by programming and interfacing a personal computer to the CMT's ESN and NAM sockets. Another approach is to interface 2 banks of 8 hexadecimal thumbwheel switches to the sockets, although a computer program would still be needed to determine the proper switch settings. Either of these two approaches would allow quick emulation of any CMT at will.

Roaming

Whenever a CMT is used in a cellular system other than the one indicated by the SID (System ID) code in its NAM, it is in the ROAM mode and the ROAM indicator on the control head will turn on. A CMT can roam in any system its home carrier has a roaming agreement with, and most carriers now have roaming agreements with each other. If there is no roaming agreement, the MTSO will transmit a recorded voice message to the CMT user with instructions to call the carrier (the only call the CMT will be able to make) and give his name, MIN, ESN, and American Express Card number. All roamed calls will then be completed by the MTSO and billed to the credit card account. Fortunately, this procedure is becoming less common as more roaming agreements are made.

Usually, a carrier can only determine if a roamer came from a system with which it has a roaming agreement, not the creditworthiness of that roamer. Consequently, many carriers have been abused by roamers who've been denied service on their home system due to non-payment. Once the home carrier is billed for roaming services provided by the roamed carrier, it will notify same to add that ESN and MIN to their MTSO's "negative verify" file to prevent further abuses. Several independent companies are establishing system software and data networks to allow Positive Roamer Verification (PRV) which will allow near real-time roamer validation by sharing data between carriers. Because of the many technical, financial, and political details that still need to be resolved, PRV systems will probably not be in place for at least two more years. In the meantime, even fictitious ESN's and MIN's can roam if they follow the standard format, although some carriers are sharing roamer data on a limited basis to prevent this.

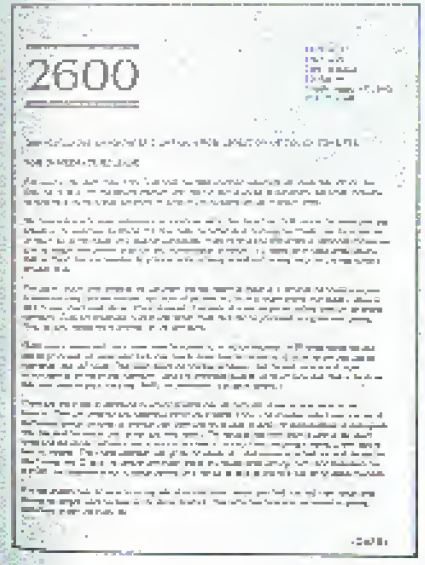
To call a roaming CMT, the caller must know which system that unit is in, and call that carrier's roaming number. Roaming numbers

(continued on page 20)

2600 Exposes New York Tel

In late June, we at *2600* got around to doing something we've been meaning to do for a long time. We've mentioned before in these pages how unfair it is that telephone companies charge consumers a monthly fee for using touch tones. They're not providing any additional service or equipment. The only real technological advance they've come up with is a device that can ignore touch tones coming from nonpaying customers. Sounds more like blackmail than a service, doesn't it?

So after having received about 25 calls from New York Telephone virtually begging us to sign up for this "service" by July so we wouldn't have to pay the "installation" fee, we reached the conclusion that enough was enough. On June 26, we mailed a press release to every newspaper, television and radio station in New York State, as well as state senators, state assemblymen, and a whole host of others we thought would be interested. Well, as it turns out, many of them were. Inside of a couple of days we were talking to all kinds of media people and it would not be an exaggeration to say that many thousands of people now know about this. The support has been terrific. Nobody likes the idea of paying a little extra every month for something that's not really there. And businesses, large and small, alike, are flabbergasted when confronted with evidence that they're paying over $4 a month per line for this non-service. Take a company with 500 lines and this comes out to $24,000 a year. Not inconsequential.


2600

And more recently, we were confronted with additional evidence of wrongdoing. It seems New York Telephone has taken to sending out undated notices informing the customer that they are about to be charged for touch tone service since touch tones were detected on their line. Many people disregard this notice because it looks just like all the other pitches they've received to sign up for touch tones. So they wind up being signed up for something they never wanted. Think about that. If touch tones were really a service, wouldn't the phone company punish a "violator" by stopping the service, rather than signing the person up for it?

We must be fair about this, however. New York Telephone is not the only telephone company doing this. But since they're local to us, we felt it only right that we tackle them first. Odds are your local company is up to the same trickery. If they are, it's up to you to make people aware of it. Call your elected officials and explain the situation to them. Keep in mind that most people accept this simply because they don't understand what's actually happening. They're thinking precisely the way the phone companies want them to. By letting people know they're being cheated and by getting them to say something about it, we're taking the most important step in reversing an unfair policy.

Letters

(continued from page 13)

understanding that you can't legally transmit data via CB radio (and, unfortunately, he lives fairly close to a Canadian Department of Communications listening post). We have thought a lot about various methods of accomplishing what we want to do, but everything seems to have some snag attached.

We have turned up some rather curious things in this quest to send free data. For example, a company called Electronic Systems Technology (1031 N. Kellogg Street, Kennewick, Washington 99336, phone (509) 735-9092) makes a device called the "ESTeem Wireless Modem". From what I can tell, this device is a cross between a Terminal Node Controller (as used by the hams) and a transceiver. It transmits on 24 channels in the frequency range of 72.040 to 72.980 mhz. It is licensed using "FCC form 574" (under "Part 90" of the FCC regulations, I believe). And when I first heard about this unit, it was being used to transmit data between the United States and Mexico. I'm told that it can be legally used in Canada as well, but what I'm not clear on is whether it can legally be used for cross-border traffic between the U.S. and Canada. Also, it appears that this unit is intended for business applications, and it seems that it might not be possible to license it for what would basically be considered "hobbyist" use (despite the transmission of the "buy/sell" messages that are forbidden on the amateur band). If you feel that I am wrong in any of these assumptions, please feel free to challenge them. In the meantime, there is one further obstacle—each wireless modem costs over $1,000! I can't imagine why the cost is so high when an amateur Terminal Node Controller/Transceiver combination can be purchased for under $400, but I can't afford one (and we'd need at least two!).

I have been told that it would be totally legal to shoot laser beams across the river. But neither of us are up on a hill (and thus "line of sight" to the other) and besides, such common local occurences as fog and very large lake freighters sailing by could easily disrupt communications.

It's really frustrating that we should have to go through all of this to try and obtain toll-free communications between two locations that are less than five miles apart. By all rights, it should be a local telephone call between Sault Ste. Marie, Michigan and Sault Ste. Marie, Ontario. But (my personal opinion follows) the Michigan Public Service Commission should be renamed the "Michigan Telephone Company Income Protection Commission", because they consistently seem to favor the interests of the telephone companies (especially Michigan Bell) over those of telephone consumers. One of their recent actions was to proclaim that there will be no new Extended Area Service areas in the state of Michigan, and that in fact, some existing Extended Area Service may be discontinued in the future (Extended Area Service is the phrase used to denote toll-free calling between telephone exchanges in nearby locations). There are other areas along the U.S./Canada border where toll-free calling is in effect between two exchanges on opposite sides of the line (Sweetgrass, Montana/Coutts, Alberta and Point Roberts, Washington/Vancouver, B.C. are two that I know of) but we are not so lucky.

In fact, not only is it a long distance call across the border, but we can't even utilize the services of any of the alternate long distance companies. With the exception of AT&T, none of

(continued on page 22)

2600 marketplace

FOR SALE: ATARI 130XE Computer, ATARI 1030 modem, 1050 disk drive, 13 inch Sharp color TV, Koala Pad, word processing, graphics and telecommunications software, manuals. Like new. Send phone # to: Box 571, Forest Hills, NY 11375.

COMMODORE 8-BIT/AMIGA USERS please send your best telecom utilities to Mark S., 11148 Burkard Ln, Rough & Ready, CA 95975. If I get enough together, I will return your disk with other people's submissions.

BEST HACKER AND PHREAKER written public domain software for the Apple II family. Two double sided diskettes full of communication and deprotection utilities. These programs were combed from the best BBS and clubs nationwide. Send $10 cash, check, or MO to Mark B., 1486 Murphy Rd., Wilmington, OH 45177-9338.

WANTED: Technical data for pay phones, dot matrix printers, and/or modems. Looking for schematics and theory of operation. Call (205) 293-5333/6395, 7 to 4 CST. Ask for Airman Parochelis. Cannot accept collect calls.

TAP BACK ISSUES—complete set (vol. 1-84) of high quality copies shipped via UPS or first class mail for $100.00. Over 400 pages of TAP material including schematics and special reports. Checks/M.O. to "P.E.I." Cash, M.O. shipped same day. SASE for sample. Pete G., P.O. Box 463, Mt. Laurel, NJ 08054.

DOCUMENTATION on electronic & digital PBX's and switching systems. Willing to trade/purchase. Also looking for Bell System Practices and other such paraphernalia. Write to Bill, c/o 2600, PO Box 752B, Middle Island, NY 11953.

32K MODEL 100, UJ-Rom II, drive, TS-DOS, spreadsheet, modem cables, AC adaptors, briefcase included, good condition, $1200. New, make an offer. Tandy 2000 version of WordPerfect 4.0 $150 or trade for 1200 or 2400 baud external modem. IBM PC & XT & AT version of WordPerfect 4.1 and MathPlan 2.1, $250 or trade for 1200 or 2400 baud external modem. Call (803) 244-6479 or (803) 233-5753. Ask for Paul.

WANTED: Looking for a good used 5 or 10 megabyte hard drive for the Apple II series of computers. If you are selling one or know of anyone that is then send replies to: Brian F., 1003 W. Main, Apt. 3, Ottawa, IL 61350.

TAIWAN! All Taiwan computers and accessories available for direct shipment for cost plus shipping plus 3% (quantities of 50 or more) Giles, PO Box 12566, El Paso, TX 79913.

I NEED INFO on a power supply made for Western Electric by ACME Electric Corp. in 1971. It is designated: Rectifier Semiconductor Type—J87233A-2 LI. Input is 208/240v, output 48v/30a using SCR's as control elements. Any info would be appreciated. A schematic would be wonderful. I'll be glad to reimburse copying costs. J. Klein, 12330 Takilma Rd., Cave Junction, OR 97523.

FOR SALE: Texas Instrument "Afeis-peruriter" (Silent 700 series) intelligent data terminal. Many uses. Reasonable. Contact Ted K., PO Box 533, Auburn, NY 13021-0533.

SCHEMATICS – BUY, SELL, TRADE. We are interested in enlarging our collection of circuit diagrams for interesting electronic devices. Send list of what you want/have and a SASE to: J.R. "Bob" Dobbs, PO Box 444, Shawnee Mission, KS 66202.

***2600* MEETINGS.** Fridays at 5 pm at the Citicorp Center in the Atrium—153 East 53rd Street, New York City. Come by, drop off articles, ask questions. We'll be in Philadelphia on July 31 at the Gallery Shopping Center. Turn page for directions. Questions? Call 516-751-2600.

GOT SOMETHING TO SELL? Looking for something to buy? Or trade? This is the place! The *2600* Marketplace is free to subscribers! Just send us whatever you want to say (without making it too long) and we'll print it! Only people please, no businesses!

Deadline for August issue: 8/5/87.

CELLULAR FRAUD

(continued from page 14)

vary, but are usually in the format: (NPA)XXX-ROAM, where NPA is the carrier's area code and XXX is the MTSO exchange. Calling that number will return a dial or ready tone, after which the roamed CMTs full MIN should be entered in Touch-Tones. After a few seconds, the mobile unit will ring or the caller will hear a recording stating that the mobile unit is out of range. Telocator Publications (202-467-4770) publishes a nationwide roaming directory for travellers with cellular phones.

Cellular Telephone technology offers phone phreaks complete safety by allowing miles of physical separation from the wire pair, and by offering thousands of lines to choose from. In addition, all this is possible from just about any location, even from a car, boat, train, or aircraft. It is these characteristics that are attracting a sophisticated new breed of phone phreaks who will enjoy unprecedented convenience and security.

catching phreaks

(continued from page 10)

800-932 800-942 800-952 800-962 800-972 800-982 800-992

(Other exchanges can be used by local phone companies—New Jersey Bell, Mountain Bell, etc.)

So for the record, don't use 800-877-8000 (US Sprint) or 800-950-1022 (MCI) illegitimately. 800-345-0007 (US Sprint) and 800-624-1022 (MCI) are much less dangerous.

(continued from page 3)

digital switching was capable of if phreaks and hackers didn't get in and show them.

Hackers have, through the help of 2600, exposed entrapment schemes that shady individuals engineered for reasons of greed and visions of glory.

In 1985, a bulletin board system belonging to 2600 was raided by law enforcement authorities on the shabbiest of pretexts. Before we were around, they would have gotten away with it without any problem. But we were able to draw attention to the absurdities and misconceptions. And the average person listened.

This month we embark on another educational campaign—proving to the average person that the phone company's touch tone fee is a farce. We have the facts and now we've attracted attention to this matter. The next couple of months will be interesting.

They'll be other campaigns in the future—and more mistruths. But, looking back on our back issues, we can see that what we've already been through hasn't been for naught.

We hope you take the opportunity to further understand our unique world by examining what are surely on the way to becoming historical relics. It certainly would give us more space to move around if you did.

Directions to the 2600 Meeting in Philadelphia at 5:00 pm in the Gallery Shopping Center.

From 30th Street Station (where Amtraks come in), go upstairs (if you've ever seen *Witness*, you may recognize the men's room) and follow the ramp to the SEPTA train towards center city. Take this train two stops to Market East. (NOTE: This ride costs $1.50 but the conductor doesn't take tickets until after Market East. So don't make it obvious where you're going and you'll get a free ride.) At Market East, go upstairs to the Gallery Shopping Center and go to the lower level. Look for people with 2600 buttons wandering around. See you there!

SAUDI ARABIAN BBS LIST

from The Veteran Cosmic Rocker

Saudi Bulletin Boards

Area	Name	Number	Speed	Protocol
Riyadh	Karavan T.B.B.S.	(01) 491 5795	3/12	8 N 1
Riyadh	Riyadh A.P.E.	(01) 464 4979 #4	3/12/24	8 N 1
Jeddah	Elyas R.B.B.S.	(02) 683 3129 #1	3/12	8 N 1
Abqaiq	Abqaiq B.B.S.	(02) 572 3884	3/12/24	8 N 1
Abu Ali	Joe's Place	(03) 578 2595	3	7 N 1
Dammam	ADC Computer Centre	(03) 825 4996	3/12	8 N 1
Dhahran	A.P.C.S. B.B.S.	(03) 873 7851	3/12	7 N 1
Dhahran	D.C.C.S. Pyramid	(03) 873 7852	3/12	8 N 1
Dhahran	Mac Maz's B.B.S.	(03) 874 0299 #2	3/12/24	8 N 1
Al Khobar	Jeraisy B.B.S.	(03) 894 7394 #3	3/12/24	8 N 1
Al Khobar	Scott Air B.B.S.	(03) 895 1643	3/12/24	8 N 1

#1 Currently available 23.00 to 09.00 and 14.00 to 17.00 Saturday to Thursday and all day Friday.

#2 Currently available 16.30 to 06.30 Saturday to Wednesday and - from 16.30 Wednesday continuously to 06.30 Saturday.

#3 Currently available 19.30 to 07.30 Saturday to Thursday and all day Friday.

#4 Currently available 18.00 to 08.00 Saturday to Thursday and all day Friday.

Letters

(continued from page 18)

the other carriers offer service here (too sparsely populated, they claim). This despite the fact that our local central office switch has been converted for "equal access". Yes, we got a ballot from Michigan Bell, with only *one* choice (AT&T, of course—I thought you only got those kind of ballots in Russia!). I guess I shouldn't complain too much—there's an area about 50 miles from here where there is no phone service at all (the folks there tried to get the MPSC to order a phone company to give them service, but the MPSC decided it was just too costly to run lines into their area, once again protecting the profits of the phone company).

The FCC recently had a proposal before it to create a "Public Digital Radio Service" that would have been just the thing for this type of application (assuming that the Canadians would have approved a similar service), but they turned it down. I'd like to know why some frequency somewhere can't be set aside for this kind of service. I hope the next time they will give us a few measly khz at least.

Perhaps there just isn't any way to do what I want to do for a reasonable cost, given the present state of legalities in the U.S. and Canada (certainly it is *technologically* possible), but if you have any suggestions, please drop me a line. Any assistance that you can provide will be very much appreciated.

JD

You seem to have really thought this out pretty carefully. Keep in mind, though, that legality is a rather hazy concept these days when it comes to electronic communications. What's legal today may not be tomorrow and may already not be in someone else's mind.

Although we'll most likely get all kinds of suggestions from our readers, these are a couple of options you may want to explore. If you can both get access to network mail through Arpanet, your friend might be able to upload what you want and you could call up later through your node and download. If you can figure out a way of linking Telenet (USA) and Datapac (Canada), you could also cut down on telephone charges, especially if you both have local dial-ups. Although PC Pursuit (the service that allows you unlimited data calls for a set fee per month) has no intention of ever going to Canada, you can trick it by dialing an alternate carrier's access number and, after waiting an appropriate amount of time, entering your authorization code and number, just as you would if you were using your own modem to place a call through an alternate carrier. This at least allows you an alternative, although it's not much of one. Also, check out the various toll-free options on alternate long distance companies—there might be a fairly cost-efficient answer there.

Finally, try being really vocal about this. Forget the computer business—call your elected officials and tell them you have a friend or relative who's only five miles away and you're sick of paying through the nose to talk to them. Apparently that worked in other towns—it seems like something could be done in your case. Make it known that the other companies refuse to serve your community. And if all else fails, you can always mail disks.

WRITE FOR *2600*!
SEND LETTERS
AND ARTICLES
TO:
2600
PO BOX 99
MIDDLE ISLAND,
NY 11953-0099